Real-Life Claims: Three Cases of Disappearing Data

How To Prepare And Protect Your Business Against Cyberattacks

VGM Insurance SERVICES

800.362.3363 | info@vgminsurance.com

Three Cases of Disappearing Data

Cyberattacks on businesses of all sizes, across all industries, are becoming more common and more impactful. As business owners and operators become more aware of these threats, malicious actors and their methods have become progressively sophisticated. Protecting your data—including your clients' health and personally identifiable information—is increasingly difficult. In fact, a study from Juniper Research found that by 2023, cyber criminals are expected to steal an estimated 33 billion records.

Frightening as the facts may be, there are ways to protect your business and your data. Let's look at three different types of cyberattacks—all based on real claims—and see what we can learn.

The Case of the Missing MFA

"What's multi-factor authentication, and why do I need it again?" you ask your IT manager, Dana. You're about to leave the office on a Friday afternoon when you remember that as part of your recent business insurance renewal, you were supposed to get multi-factor authentication (MFA) in place for your business network before the new policy takes effect—which is Tuesday next week!

"It adds an extra layer of security to our network," Dana says. "It means if someone steals your username and password, they still won't be able to get in. It's important protection for our client data. We'll need to get some kind of third-party app or software to set it up."

"Oh, that sounds expensive," you say. "Remind me to look into that right away on Monday."

The weekend passes, and Dana gets involved in a new project the following week. She forgets all about your conversation. You forget too.

Fast forward two months. Your new business insurance policy is in effect, and you still don't have MFA protection. Everything is fine until you try to log on to your computer one sunny Wednesday morning and see a "YOUR FILES ARE ENCRYPTED" message on the screen. You restart your computer, and the same message appears. You look around, half expecting it to be a joke, but as you see the pale faces of your team, you realize there is nothing to laugh about. You're locked out of everything. Your business cannot function. This is not a drill.

Eventually, Dana and the team get your system back up and running without having to pay anything to cybercriminals. But you're not in the clear. Your business was entirely down for six days, and your client data was compromised.

You're relieved to remember you have Cyber Liability coverage, but there's one problem. You never implemented MFA, so your policy is considered void. Not only do you have to notify your clients of their compromised data—you also must absorb six days of losses. You're honestly not sure your business will survive this devastating financial hit.

The Case of the Software Snafu

You love your business management software. You use it for everything—patient appointments, billing, and documentation. You pay plenty to the third-party software vendor, but it's worth every penny. You don't know how you'd run your business without it.

Turns out, you actually can't run your business without the software, and you learn this the hard way. The software vendor is hacked, and all your patient data is compromised. Not only that, you can't access your patient contact information, or even see the schedule to know what appointments you need to cancel. What's more, the vendor closes for four days to fix the problem. You have no choice but to close your business as well.

You're so relieved to have a Cyber Liability policy, but you really thought you'd never need it. You'd assumed the vendor's coverage would have protected your business in a case like this. Your own policy is basic, and the coverage limits are low. Too low to come close to covering your losses. That's money you'll never see again.

The Case of the Phishy Funds Transfer

You are worried about the prevalence of cyberattacks, so you invest in training for your staff, as well as a Cyber Liability policy. In your mind, you've checked all the boxes for being cyber-safe, and you feel good about the steps you've taken to protect your business.

That's why you're shocked when the entire month's payroll suddenly disappears from your company's bank account. It turns out your HR department received an email from the CFO asking them to change deposit accounts for payroll. The email looked real, and there were none of the red flags they've been taught to look for. The sender's email address looked legitimate. There were no typos, spelling errors, or anything else to tip them off.

Deciding to avoid a potentially awkward confrontation, the payroll team went ahead and changed the direct deposit information as requested. And the money disappeared.

It turns out that not only were the payroll funds lost for good, but Funds Transfer Fraud as this kind of cyber crime is labeled, was NOT included in your Cyber Liability policy. You wish you'd thought to examine your policy closer and discuss it with your agent. You'd just assumed you'd be covered for any kind of cyber incident.

Best Practices to Protect Against Cyber Threats

While it's impossible to completely avoid being impacted by a cyberattack, there are proactive steps you can take to lower your risk, and be prepared in case an attack does occur on your business, or a third-party you work with. Here are some things the businesses in these scenarios could have done, and things you can do to help make sure you're as prepared as possible.

Implement MFA

Our first case may not have been preventable, but the business owner could have had their losses covered if they'd only implemented multi-factor authentication. MFA or 2FA is not only crucial to protect against cyberattacks, but also to securing adequate insurance coverage. While MFA used to be optional or "nice to have," it is now essential. Most insurance carriers are now requiring businesses to have it to write or renew their Cyber Liability policies. There are many simple and affordable solutions available. Ask your insurance provider for their recommendations.

MFA works by requiring more than just a username and password to log into your systems or network. For instance, you'll need to add a phone number or security code. You may even need to add a time-based one-time password (TOTP), automatically generated by an authenticator app. This extra level of protection makes it much harder for cyber criminals to gain access to your network. It's especially effective against ransomware, the most common type of cyberattack.

Ensure Adequate Insurance Coverage

In the second case, there was no way for the business owners to mitigate their cyber risk. Most businesses use a third-party vendor for at least one essential operation, and if the vendor is the victim of a cyberattack, you are too. As the business owner in the story discovered, it is not enough to make sure you have Cyber Liability coverage in place. You also need to make sure that your coverage is adequate to meet the needs of your business. Meet with your insurance provider to review your coverage and ensure the limits and types of coverage you have in place are sufficient to withstand even a large-scale attack.

Review Your Policy for Exclusions

Both the second and third case studies demonstrate how critical it is to know what your policies cover. Many policies have exclusions and exceptions, and those apply whether you know about them or not. It's important to know what's not covered and what you are saying "no" to. Carefully review your policy with your insurance provider to see if you need to purchase additional policies to protect against certain kinds of cyber events.

Beware of Phishing Attacks

Our business owner in the third case study thought they'd done everything right, but even the most well-meaning, proactive businesses and employees can fall victim to phishing attacks. Remember that cybersecurity training is an ongoing endeavor. Provide employees with regular, timely training about how to spot a phishing attack and provide clear instructions on what to do with suspicious emails. Phishing attacks are becoming increasingly sophisticated and harder to spot. Train your employees that it's always better to double-check the source of *any* email than to click or take an action they may later regret. It's far less embarrassing to ask someone to confirm an email they sent than it is to be responsible for a cyberattack.

For more best practices to follow, see this ***Ransomware Checklist***.

For more information about how you can minimize cyber risks for your business, and to ensure you have adequate coverage, reach out to your VGM Insurance Account Manager or contact us today at ***info@vgminsurance.com*** or ***800-362-3363***.

Through our sister company, ***VGM Forbin***, we also provide access to an affordable multi-factor authentication (MFA) software called Duo. Contact Senior IT Analyst Nick Dideriksen at **nickd@forbin.com** or ***855-755-6952*** to learn more and get MFA set up for your business.

VGM Insurance SERVICES